	Application No.	Applicant(s)
Notice of Allowability	09/306,110	HASEGAWA, SATOSHI
	Examiner	Art Unit
	Christopher A. Revak	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the communication filed on 9/15/05.*

2. ☒ The allowed claim(s) is/are *1,2,4-9,11 and 14-17.*

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☒ All   b) ☐ Some*   c) ☐ None of the:

      1. ☒ Certified copies of the priority documents have been received.

      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .

      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

    * Certified copies not received: _____ .

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.

    (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached

      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____ .

    (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____ .

    Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)

2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)

3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____

4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material

5. ☐ Notice of Informal Patent Application (PTO-152)

6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .

7. ☒ Examiner's Amendment/Comment

8. ☒ Examiner's Statement of Reasons for Allowance

9. ☐ Other _____ .

Primary Examiner
AU 2131
11/29/05

NOTICE OF ALLOWANCE

Examiner's Amendment

1.   An examiner's amendment to the record appears below. Should the changes

and/or additions be unacceptable to applicant, an amendment may be filed as provided

by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be

submitted no later than the payment of the issue fee.

The application has been amended as follows:

In claim 17, line 5, delete –astream- and replace with "a stream".

Allowable Subject Matter

2.   Claims 1,2,4-9,11, and 14-17 are allowed based upon the applicant's arguments.

3.   The following is an examiner's statement of reasons for allowance:

As per claim 1, it was not found to be taught in the prior art of a stream buffer for

temporarily storing a calculated data stream and inverse calculation means for

performing an inverse calculation on the calculated stream output from the stream

buffer by using a variable to reproduce the data stream. The variable is changeable at

regular timing or random timing.

As per claim 5, it was not found to be taught in the prior art of a stream buffer for

temporarily storing a calculated data stream and inverse calculation means for

performing an inverse calculation on the calculated stream output from the stream

buffer to reproduce the data stream. The variable is changeable at regular timing or

random timing. A variable creation means is used for creating a number of variables where a variable is arbitrarily chosen as the variable used for the calculation.

As per claim 8, it was not found to be taught in the prior art of a stream buffer for temporarily storing a calculated data stream and inverse calculation means for performing an inverse calculation on the calculated stream output from the stream buffer by using a variable to reproduce the data stream. Variable creation means creates a variable set consisting of a number of variables and a variable is selected from the variable set to perform a calculation on the data stream.

As per claim 15, it was not found to be taught in the prior art of a stream buffer for temporarily storing a calculated data stream and inverse calculation means for performing an inverse calculation on the calculated stream output from the stream buffer by using a variable to reproduce the data stream. Variable designation means designates the variable that is periodically changed per each clock cycle.

As per claim 16, it was not found to be taught in the prior art of a stream buffer for temporarily storing a calculated data stream and inverse calculation means for performing an inverse calculation on the calculated stream output from the stream buffer by using a variable to reproduce the data stream. The variable used for the inverse calculation is updated in conformity with a variable update timing inserted into the data stream.

As per claim 17, it was not found to be taught in the prior art of a stream buffer for temporarily storing a calculated data stream and inverse calculation means for performing an inverse calculation on the calculated stream output from the stream

buffer by using a variable to reproduce the data stream. The variable is changeable at regular timing or random timing.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

4.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Feistel, U.S. Patent 4,316,055 is a basic teaching of stream ciphers.

Kitani et al, US 2004/0006703 discloses of a seed value that is an initial input value for a random number generator that corresponds to a common key used for encrypting streams.

5.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-3:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
Primary Examiner
AU 2131

CR

November 29, 2005